Switch

Switch EV Ltd comments on the Notice of Proposed Rulemaking (NPRM) for the National Electric Vehicle Infrastructure (NEVI) Formula Program

Comments on Docket No. FHWA-2022-0008

Date: August 22, 2022

Switch has reviewed the proposed set of minimum standards and requirements for NEVI Formula Program projects and projects for the construction of publicly accessible EV chargers that are funded under title 23, United States Code.

We appreciate that the NEVI Formula Program mandates ISO 15118 in combination with OCPP 2.0.1 as a set of minimum standards for a future-proof, publicly funded DC fast charger network in the US.

We'd like to raise the following comment to bring further clarity into the proposal and avoid any remaining ambiguity as to the mandated protocols under this program:

1. The specific OCPP version 2.0.1 should be mentioned across the document instead of referring only to OCPP in the majority of cases. Only section 680.120 Reference Manuals clarifies which OCPP version NEVI proposes to use. We need to avoid any doubt and ambiguity about the OCPP version. It needs to be very clear that OCPP 1.6 chargers will not be funded by the NEVI program because it does not satisfy the need for
    a. secure communication to mitigate cybersecurity risks (e.g. OCPP 1.6 does not provide mutual TLS authentication with digital certificates between charger and backend and does not enable secure firmware updates);
    b. seamless Plug and Charge (only OCPP 2.0.1 has been developed to specifically accommodate ISO 15118 data structures and messages);
    c. advanced charger diagnostics through the new Device Model concept.

    Given that the NPRM also specifically points to OCPI version 2.2.1, we should do the same with OCPP 2.0.1.

2. Add ISO 15118-20 in the list of published ISO 15118 standards, as Part 20 was published in April 2022. Chargers need to be equipped with the minimum resources to handle both ISO 15118-2 and -20 and store all relevant certificates and private key material. In two years' time at the latest, we'll see the first -20 compatible,

V2G-enabled EVs on the market. The chargers need to be ready for it, even if V2G is not a specific use case for DC fast chargers. ISO 15118-20 also brings stronger data security through updated cipher suites that help mitigate cybersecurity risks.

Here's a snippet of a slide presentation from Germany-based Vector on the cybersecurity changes in ISO 15118-20 and the effect on the ROM in EVs. Certificate sizes doubled from 800 bytes to 1600 bytes and the amount of certificates that need to be stored also increased. New future-proof cipher suites are being introduced to elevate cybersecurity protection against malicious third parties.

If EV charger manufacturers are not made aware of these new requirements, then the charging infrastructure put in the ground and subsidised by the NEVI program might not be future-proofed enough.

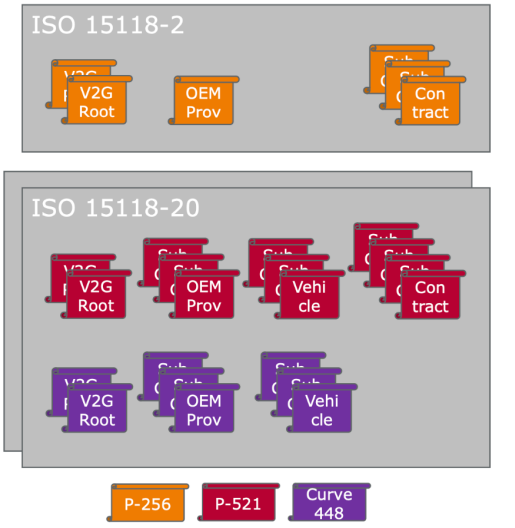
Increased Complexity of ISO 15118-20

VECTOR

Certificate "Infrastructure"

- Maximum size of X509v3 certificate increased from 800 to 1600 bytes
- Cross-signing was introduced
  - Maximum chain length increased from 3 to 4
  - Cross-signing may require two parallel Sub CA 1
- ISO 15118-20 supports P-521 and Curve448
  - Most certificates stored once for each curve
  - P-521 is default curve
  - Curve448 is only backup
    - In case P-521 will get compromised
- ISO 15118-2 required for backwards compatibility

- Example calculation for ROM
  - ISO 15118-2: 6*800 Bytes = 4800 Bytes
  - ISO 15118-20: 20*1600 Bytes = 32,000 Bytes
  - Overall: 36,800 Bytes



Switch

Increased Complexity of ISO 15118-20

VECTOR

Impact on Cryptography

	ISO 15118-2	ISO 15118-20
TLS Version	1.2	1.3
Client Authentication	No	Yes
Cipher Suites	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Curves	P-256	P512 (default) Ed448 (backup)
Key Agreement	ECDHE (forward secrecy) ECDH	ECDHE (forward secrecy)
Symmetric Encryption	AES 128 CBC	AES 256 GCM
Hash Algorithm	SHA256	SHA256 SHA384 SHA512 (XML Signatures) SHAKE256 (XML Signatures)
Signature Algorithms	ecdsa-sha256	ecdsa_secp521r1_sha512 Ed448 (Curve448 with SHAKE256)
Dedicated TPM Support	No	Yes

3. Uptime: It is not 100% clear whether or not a lost link, and therefore lost websocket connection between EV charger and backend, would be counted as downtime. It seems that the current wording regards a charger that is temporarily disconnected from the backend but still provides electricity to the EV through offline authorisation as being “up”. However, it remains slightly ambiguous. Please clarify.

4. Currently, there are companies that talk about enabling “Plug and Charge” but what they really mean is Autocharge (authentication based on MAC address, not an ISO 15118 digital certificate). Please clarify in your “Section 680.104 Definitions” that Plug and Charge is meant as defined in the ISO 15118 standard, using digital certificates.

5. §680.108 Interoperability of electric vehicle charging infrastructure: Should not only reference ISO 15118 but also OCPP 2.0.1 as both are relevant for interoperability of EV charging infrastructure.

Kind regards

Marc Mültin
CEO & Founder Switch EV Ltd